

**SEALED**CLERK'S OFFICE U.S. DIST. COURT  
AT CHARLOTTESVILLE, VA  
FILED

AUG 25 2017

IN THE UNITED STATES DISTRICT COURT FOR THE  
FOR THE  
WESTERN DISTRICT OF VIRGINIA  
CHARLOTTESVILLE DIVISIONJULIA C. DUDLEY, CLERK  
BY:  DEPUTY CLERKIN THE MATTER OF A SEARCH OF:  
)  
)  
INFORMATION ASSOCIATED WITH  
VOLKERIL@OUTLOOK.COM;  
AMERIKAN-STEEL@OUTLOOK.COM;  
STORED AT PREMISES CONTROLLED  
BY MICROSOFT  
)  
)

Case No. 3:17-mj-00046

UNDER SEAL**AFFIDAVIT IN SUPPORT OF AN APPLICATION  
FOR A WARRANT TO SEARCH AND SEIZE**

I, Christopher Hartley, being duly sworn, depose and state as follows:

**INTRODUCTION**

1. I am a Special Agent of the United States Department of Justice, Federal Bureau of Investigation ("FBI") and have been so employed since February 2016. I am assigned to the Washington Field Office, Northern Virginia Resident Agency, located in Manassas, Virginia. My principal duties include the investigation of, among other matters, civil rights violations of the United States.

2. I am a federal law enforcement officer under applicable provisions of the United States Code under Rule 41(a) of the Federal Rules of Criminal Procedure. I have received training in and have experience in the enforcement of the laws of the United States, including the preparation and presentation of search warrants, and in executing court-ordered search warrants.

3. I make this affidavit in support of an application by the United States of America for a warrant to search and seize evidence associated with Microsoft Outlook accounts: **volkeril@outlook.com** and **amerikan-steel@outlook.com**, as further described in Attachment A.

4. Based on the information below, I submit there is probable cause to believe the aforementioned Outlook accounts will contain evidence, as more fully identified in Attachment B, of violations of federal law, including, but not limited to, Title 18, United States Code, Section 249 (Hate Crime).

5. Through training and experience, the Affiant has knowledge that domestic terrorists and persons affiliated with white supremacists group and/or conspirators will utilize cell phones, and other electronic devices, electronic mail ("E-mail"), and social media to conduct their illegal activity and maintain contact with other confederates, conspirators and criminal associates involved with the planning, targeting, and execution of their political or social goals to include, but not limited to, espousing violence.

6. The Affiant bases this affidavit upon personal knowledge and observations made during the course of this investigation, information conveyed to me by other law enforcement officers assigned to this investigation, and upon my personal review of records, documents, and items lawfully obtained by third parties. This affidavit is not intended to include each and every fact known to me or the other investigating agencies, nor does it reflect all the evidence developed during the course of the investigation. Instead, the Affiant has set forth sufficient information to establish probable cause for the issuance of the requested search warrant. Where the contents of documents and the actions, statements and conversations of others are reported herein, they are reported in substance and in part.

### **RELEVANT STATUTE**

7. Title 18, United States Code, Section 249, provides that “Whoever, whether or not acting under color of law, willfully causes bodily injury to any person or, through the use of fire, a firearm, a dangerous weapon, or an explosive or incendiary device, attempts to cause bodily injury to any person, because of the actual or perceived race, color, religion, or national origin of any person” shall be guilty of a federal offense.

### **JURISDICTION**

8. This Court has jurisdiction to issue the requested warrant because it is “a court of competent jurisdiction” as defined by 18 U.S.C. § 2711. 18 U.S.C. §§ 2703(a), (b)(1)(A) & (c)(1)(A). Specifically, the Court is “a district court of the United States . . . that – has jurisdiction over the offense being investigated.” 18 U.S.C. § 2711(3)(A)(i).

### **BACKGROUND**

9. On August 12, 2017, a “Unite the Right” rally was held at Emancipation Park in Charlottesville, Virginia. The proclaimed purpose of the rally was to protest the removal of the Robert E. Lee and Thomas “Stonewall” Jackson statues in Charlottesville, Virginia. Several groups espousing right-wing nationalist and/or white supremacist views attended the rally in support.

10. In addition, several thousand counter-protestors attended the rally to oppose the rally and its supporters. Throughout the day, several instances of violence occurred between protestors and counter-protestors. At approximately noon, the rally was declared an unlawful assembly by the Charlottesville Police Department, and both protestors and counter-protestors dispersed to separate locations.

11. A group observed by law enforcement at the aforementioned rally was Vanguard America, whose beliefs are stated as:

*"The chains of debt slavery wrap themselves tight around White Americans, such conditions must be reversed. A new generation of corporate leaders, who hold the interests of White America first and foremost, will naturally rise to the top of this new economy."*

Below is a picture of the Vanguard America emblem taken from the website

<https://bloodandsoil.org/>:



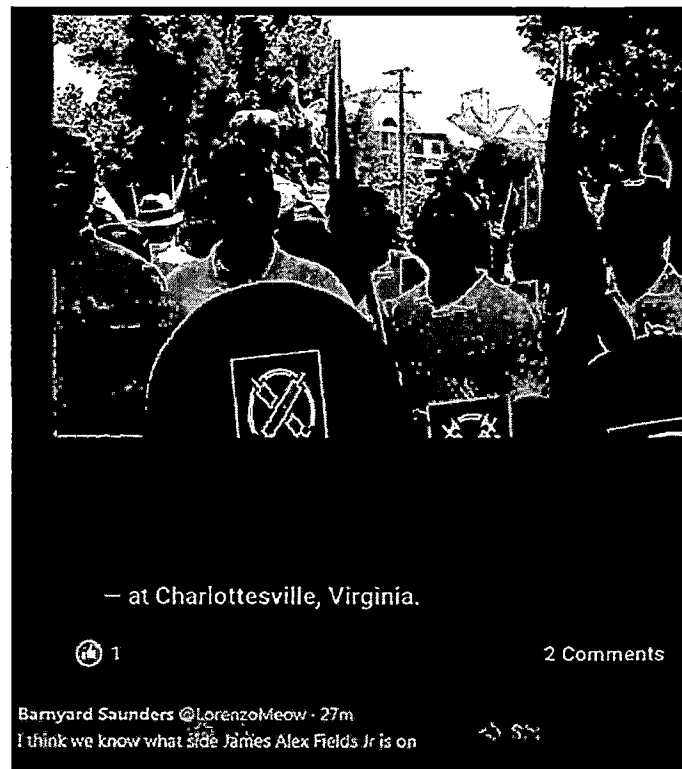
The right-wing nationalist slogan "blood and soil" is derived from a German phrase, used by Adolph Hitler's Nazis, that purportedly promotes the notion that people with "white blood" are uniquely connected to "American soil."

#### **PROBABLE CAUSE**

12. The FBI is conducting an investigation into possible violations of federal criminal law committed by JAMES ALEX FIELDS ("FIELDS"), an individual allegedly associated with Vanguard America and other white supremacist groups. The investigation was initiated following receipt of information FIELDS drove this vehicle, a grey Dodge Charger bearing Ohio license plate GVF1111, into a crowd of people during the "Unite the Right Rally" in Charlottesville, Virginia on August 12, 2017. The incident killed one Caucasian female and injured approximately twenty-eight (28) other individuals of African-American and Caucasian descent.

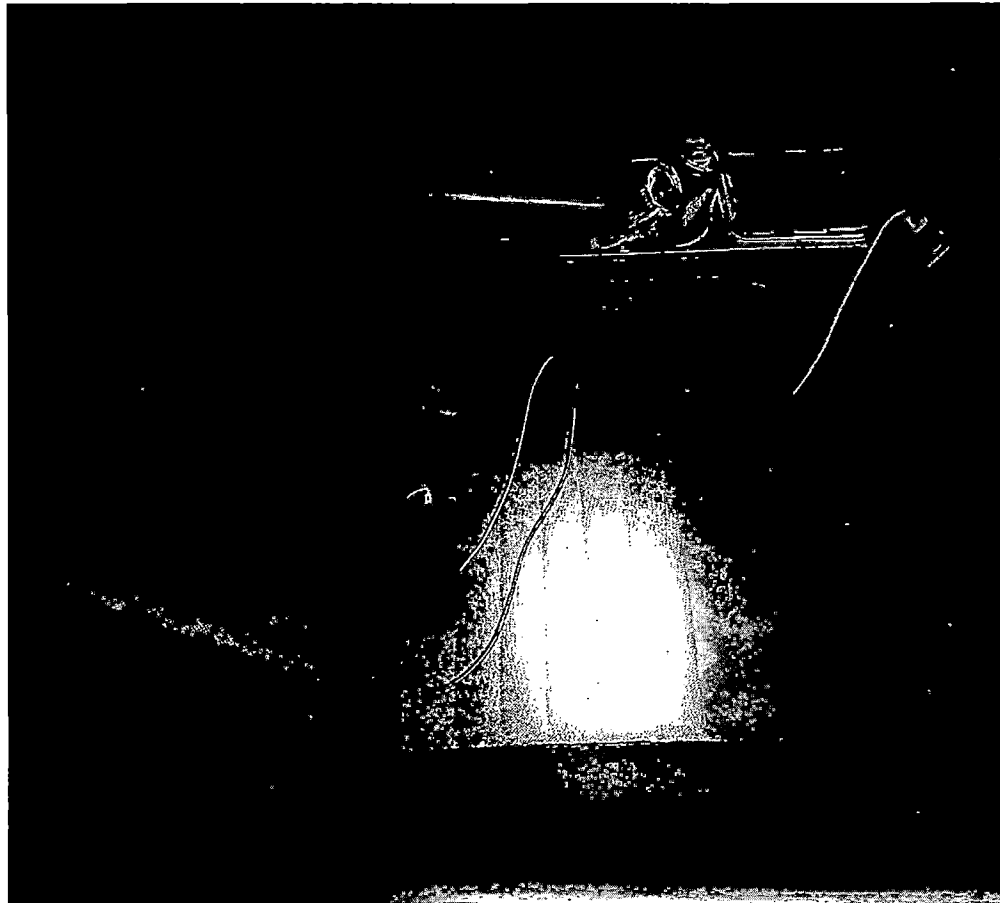
13. Based on Affiant's review of the video footage of the incident, FIELDS' vehicle travelled at a high rate of speed and intended to strike rally counter-protestors, including African-Americans. After striking multiple victims with his vehicle, FIELDS drove his vehicle backwards, in reverse, at high-rate of speed to flee the scene.

14. After his arrest by the Charlottesville Police Department, FIELDS was observed dressed in a white polo shirt, khaki pants, and black shoes. FIELDS' hair was trimmed with a "high and tight" or "side-fade" style consistent with the hair style of other individuals associated with the white supremacist group Vanguard America at the rally. Below is a picture of FIELDS that law enforcement officials obtained from social media at the Charlottesville "Unite the Right" rally. Fields is second person from the left with the large black shield in front of him.



15. The Affiant learned from law enforcement officials and review of video footage, one individual was in the vehicle at the time of the aforementioned incident. After the

Charlottesville Police arrested FIELDS, his vehicle was towed and stored in a secured law enforcement facility.



16. On August 12, 2017, the FBI interviewed SAMANTHA BLOOM ("BLOOM"), a woman identified as FIELDS' mother. BLOOM confirmed details about FIELDS and his trip to Charlottesville, Virginia for the "Unite the Right" rally. According to the BLOOM, she knew this information from a text message sent to her from FIELDS.

17. BLOOM consented to showing FIELDS' contact information in her, BLOOM'S, phone. The contact information displayed FIELDS known phone number as 859-414-9660 and e-mail address as **Volkeril@outlook.com**.

18. In addition, e-mail address **amerikan-steel@outlook.com** was listed as a point of contact by FIELDS on his Ohio Driver's License application.

19. Microsoft provides email services with the domain names hotmail.com, live.com, and outlook.com, which are available free of charge to Internet users. Subscribers obtain an account by registering via the Internet with Microsoft;

20. Microsoft maintains electronic records pertaining to the individuals and companies for which they maintain subscriber accounts. These records include account access information, email transaction information, and account application information as well as the other items more specifically detailed in Attachment A. In my training and experience, email providers typically retain certain transactional information about the creation and use of each account on their systems. This information can include the date on which the account was created, the length of service, records of log-in (i.e., session) times and durations, the types of service utilized, the status of the account (including whether the account is inactive or closed), the methods used to connect to the account (such as logging into the account via the provider's website), and other log files that reflect usage of the account. In addition, email providers often have records of the Internet Protocol address ("IP address") used to register the account and the IP addresses associated with particular logins to the account. Because every device that connects to the Internet must use an IP address, IP address information can help to identify which computers or other devices were used to access the email account.

21. In my training and experience, email providers generally ask their subscribers to provide certain personal identifying information when registering for an email account. Such information can include the subscriber's full name, physical address, telephone numbers and other identifiers, alternative email addresses, and, for paying subscribers, means and source of payment

(including any credit or bank account number). In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the account's user or users. Based on my training and my experience, I know that even if subscribers insert false information to conceal their identity, I know that this information often provide clues to their identity, location or illicit activities;

22. Subscribers to Microsoft email can access their accounts on servers maintained and/or owned by Microsoft from computers connected to the Internet around the world;

23. A Microsoft email user seeking to send email can use a web-based interface to log into the account, type the message, and then submit it to Microsoft's mail servers for transmission to its recipient(s). Similarly, a Microsoft email user seeking to read a received message can use a web-based interface to log into the account and view the message on Microsoft's servers;

24. A Microsoft subscriber may elect to download and store on his or her personal computer copies of email messages or other files sent or received via the account. In addition to, or instead of, downloading such data to a local computer, a Microsoft email user may elect to remotely store copies of email messages or other files sent or received via the account on Microsoft's servers for subsequent retrieval. Accordingly, a search of the files in the computer in the subscriber's residence will not necessarily uncover the files that the subscriber has stored on the Microsoft server—and vice versa;

25. In my training and experience, in some cases, email account users will communicate directly with an email service provider about issues relating to the account, such as technical problems, billing inquiries, or complaints from other users. Email providers typically retain records about such communications, including records of contacts between the user and the provider's support services, as well records of any actions taken by the provider or user as a result



of the communications. In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the account's user or users.

26. As explained herein, information stored in connection with an email account may provide crucial evidence of the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, the information stored in connection with an email account can indicate who has used or controlled the account. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. For example, email communications, contacts lists, and images sent (and the data associated with the foregoing, such as date and time) may indicate who used or controlled the account at a relevant time.

27. Further, information maintained by the email provider can show how and when the account was accessed or used. For example, as described below, email providers typically log the Internet Protocol (IP) addresses from which users access the email account along with the time and date. By determining the physical location associated with the logged IP addresses, investigators can understand the chronological and geographic context of the email account access and use relating to the crime under investigation. This geographic and timeline information may tend to either inculcate or exculpate the account owner. Additionally, information stored at the user's account may further indicate the geographic location of the account user at a particular time (e.g., location information integrated into an image or video sent via email). Last, stored electronic data may provide relevant insight into the email account owner's state of mind as it relates to the offense under investigation. For example, information in the email account may indicate the

owner's motive and intent to commit a crime (e.g., communications relating to the crime), or consciousness of guilt (e.g., deleting communications in an effort to conceal them from law enforcement).

28. As a federal agent, I am trained and experienced in identifying communications relevant to the crimes under investigation. The personnel of Microsoft may not be. I also know that the manner in which the data is preserved and analyzed may be critical to the successful prosecution of any case based upon this evidence. Computer Forensic Examiners are trained to handle digital evidence. Microsoft employees may not be. It would be inappropriate and impractical, however, for federal agents to search the vast computer network of Microsoft for the relevant accounts and then to analyze the contents of those accounts on the premises of Microsoft. The impact on Microsoft's business would be severe;

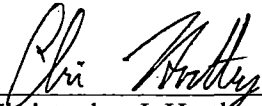
29. In order to accomplish the objective of the search warrant with a minimum of interference with the business activities of Microsoft, to protect the rights of the subject of the investigation and to effectively pursue this investigation, authority is sought to allow Microsoft to make a digital copy of the entire contents of the information subject to search specified in Attachment A. That copy will be provided to me or to any authorized federal agent. The contents will then be analyzed to identify records and information subject to seizure pursuant to Attachment A; and

30. Executing a warrant to search a Microsoft email account requires an approach similar to the standard approach for executing a warrant to search papers stored in a file cabinet. Searching the subject email account in this case for evidence of the target crimes will require that agents cursorily inspect all emails produced by Microsoft in order to ascertain which contain evidence of those crimes, just as it necessary for agents executing a warrant to search a filing

cabinet to conduct a preliminary inspection of its entire contents in order to determine the documents which fall within the scope of the warrant. In addition, keyword searches alone are inadequate to ensure that law enforcement can discover all information subject to seizure pursuant to Attachment A. Keywords search text, but many common electronic mail, database and spreadsheet applications files (which files may have been attached to electronic mail) do not store data as searchable text.

**CONCLUSION**

31. Based on the forgoing, I request that the Court issue the proposed search warrant. Because the warrant will be served on Microsoft who will then compile the requested records at a time convenient to it, reasonable cause exists to permit the execution of the requested warrant at any time in the day or night.

  
\_\_\_\_\_  
Christopher J. Hartley  
Special Agent  
Federal Bureau of Investigation

Subscribed and sworn before me this 25<sup>th</sup> of August, 2017.

  
\_\_\_\_\_  
United States Magistrate Judge